BOLETIM DA REPÚBLICA

PUBLICAÇÃO OFICIAL DA REPÚBLICA DE MOÇAMBIQUE

IMPRENSA NACIONAL DE MOÇAMBIQUE, E.P.

AVISO

A matéria a publicar no «Boletim da República» deve ser remetida em cópia devidamente autenticada, uma por cada assunto, donde conste, além das indicações necessárias para esse efeito, o averbamento seguinte, assinado e autenticado: **Para publicação no «Boletim da República».**

SUMÁRIO

BANCO DE MOÇAMBIQUE

Aviso n.º 4/GBM/2015

de 17 de Junho

A Lei n.º 14/2013, de 12 de Agosto, estabelece o novo regime de Prevenção e Combate ao Branqueamento de Capitais e Financiamento ao Terrorismo em Moçambique e, de entre outros aspectos, atribui às autoridades de supervisão competência para emitir normas para materializar o cumprimento da lei.

Mostrando-se necessário orientar a actuação das instituições financeiras, que nos termos da referida Lei se encontram sob sua alçada de supervisão, o Banco de Moçambique, usando das competências que lhe são atribuídas pelas disposições conjugadas das alíneas *a*) do artigo 27 e alíneas *b*) e *c*) do n.º 2 do artigo 29 da referida Lei, determina:

1. São aprovadas as Directrizes sobre Prevenção e Repressão do Branqueamento de Capitais e Financiamento ao Terrorismo, em anexo ao presente Aviso, que dele faz parte integrante.

2. O incumprimento das normas do presente Aviso constitui contravenção punível nos termos da Lei n.º 14/2013, de 12 de Agosto.

3. O presente Aviso entra em vigor 60 (sessenta) dias após a sua publicação, revogando todas as disposições em contrário.

As dúvidas que surgirem na interpretação e aplicação do presente Aviso devem ser submetidas ao Departamento de Regulamentação e Licenciamento do Banco de Moçambique.

Maputo, 6 de Maio de 2015. — O Governador do Banco de Moçambique, *Ernesto Gouveia Gove*.

Directrizes Sobre Prevenção e Repressão do Branqueamento de Capitais e Financiamento ao Terrorismo

CAPÍTULO I

Objecto e âmbito de aplicação

1. As presentes directrizes estabelecem os procedimentos e medidas de prevenção e repressão ao branqueamento de capitais e financiamento ao terrorismo.

2. As presentes directrizes aplicam-se a todas as instituições financeiras que, ao abrigo das alíneas *a*), *b*) e *d*) do n.º 2 do artigo 3 e da alínea *a*) do artigo 27 da Lei n.º 14/2013, de 12 de Agosto, se encontram sob supervisão do Banco de Moçambique.

3. As instituições financeiras de espécie diferente de bancos e microbancos estão sujeitas às normas do presente Aviso, na parte que lhes seja aplicável.

CAPÍTULO II

Programa de Controlo Interno

SECÇÃO I

Responsabilidades do Conselho de Administração ou equiparado

1. O Conselho de Administração ou órgão com funções equiparadas das instituições financeiras deve documentar e aprovar as políticas sobre identificação, avaliação e gestão de risco e medidas de controlo interno que permitam gerir e mitigar eficazmente, privilegiando uma abordagem baseada no risco, os riscos de branqueamento de capitais e financiamento do terrorismo identificados.

2. O Conselho de Administração ou órgão equiparado deve garantir que o processo de controlo e os procedimentos adoptados são eficazes, efectivos e contribuem para a redução do risco de a instituição ser usada para fins de branqueamento de capitais e financiamento ao terrorismo.

3. A política de gestão de risco de branqueamento de capitais e financiamento ao terrorismo deve conter, nomeadamente:

a) Políticas e procedimentos sobre o dever de identificação e verificação, que, no mínimo, contemplem: política de aceitação de clientes, procedimentos de identificação e monitoramento das transacções suspeitas;
b) Políticas e procedimentos sobre a avaliação, gestão de risco e procedimentos de monitoria;
c) Políticas sobre o sigilo relativo às contas que se encontram sob monitoramento para determinar transacções suspeitas;
d) Políticas e procedimentos internos sobre o reporte de transacções suspeitas e outros tipos de reportes;
e) Políticas e procedimentos internos sobre a conservação de documentos.

4. O Conselho de Administração ou órgão equiparado deve ainda nomear, para sede, agências, filiais, sucursais e outras formas de representação da instituição, um Oficial de Comunicação de Transacções Suspeitas (OCOS). O OCOS deve ser escolhido de entre os funcionários de nível de gestão da instituição, devendo, no mínimo, exercer as atribuições referidas no n.º 2 deste Capítulo.
5. O Conselho de Administração ou órgão equiparado deve assegurar recursos suficientes para a funcionalidade do OCOS, nomeadamente recursos humanos, materiais e tecnológicos. O nível dos recursos deve reflectir a dimensão, complexidade, número de clientes e produtos oferecidos pela instituição.

SECÇÃO II

Responsabilidades do OCOS

1. O OCOS suporta e orienta a gestão do risco de branqueamento de capitais e financiamento ao terrorismo na instituição financeira.
2. Sem prejuízo do estabelecido em demais legislação aplicável, são responsabilidades do OCOS, nomeadamente:

a) Garantir o envio de reportes de transacções suspeitas ao Gabinete de Informação Financeira de Moçambique (GIFiM), com toda a informação relevante sobre a transacção e o cliente;
b) Garantir o envio imediato de toda a informação adicional solicitada pelas autoridades competentes no âmbito de casos suspeitos de branqueamento de capitais e financiamento ao terrorismo;
c) Rever com regularidade a adequação do sistema de controlos sobre a prevenção e combate ao branqueamento de capitais e financiamento ao terrorismo, nomeadamente fiscalizando a implementação das políticas e procedimentos para a prevenção e combate ao branqueamento de capitais e financiamento ao terrorismo, assegurando um processo de monitoramento apropriado e participando de forma activa na escolha da aplicação informática (*software*) para monitorar os clientes e suas transacções;
d) Assegurar a coordenação com as várias partes interessadas, nomeadamente os auditores internos, os auditores externos, o Banco de Moçambique, o GIFiM e as autoridades judiciais;
e) Garantir que toda a informação relevante sobre a prevenção do branqueamento de capitais e financiamento ao terrorismo seja transmitida aos trabalhadores, fiscalizando o cumprimento das políticas sobre a formação e capacitação aprovada pela instituição e assegurando que o seu conteúdo seja adequado, actual e se encontre alinhado com as boas práticas e as tendências dos contornos do fenómeno de branqueamento de capitais e financiamento ao terrorismo.

SECÇÃO III

Responsabilidade da auditoria interna

1. A auditoria interna é responsável pela realização de uma avaliação independente e pela eficácia e eficiência do sistema de prevenção do branqueamento de capitais e financiamento ao terrorismo, devendo nomeadamente verificar a adequação das políticas, procedimentos e suporte do sistema para detectar potenciais operações suspeitas de branqueamento de capitais e financiamento ao terrorismo.
2. O relatório de auditoria interna deve ser remetido, em tempo útil, ao conselho de administração e ao comité de auditoria, havendo-o.
3. O programa de auditoria interna deve estar alinhado com a avaliação do risco efectuado pela instituição financeira.

CAPÍTULO III

Dever de identificação e verificação

SECÇÃO I

Conheça o seu Cliente

As instituições financeiras devem adoptar políticas sobre a identificação e verificação dos seus clientes. A política do "conheça o seu cliente", das instituições financeiras, deve incorporar os seguintes elementos:

a) Política de aceitação de clientes;
b) Os procedimentos de identificação e verificação do cliente;
c) Monitoramento de operações; e
d) Gestão de riscos.

SECÇÃO II

Política de aceitação de clientes

1. As instituições financeiras devem elaborar uma política clara sobre a aceitação de clientes, incluindo medidas aplicáveis para cada categoria de clientes.
2. A política de aceitação de clientes deve ter em conta riscos associados ao cliente, ao País ou à região geográfica e riscos associados ao canal de entrega do produto, ao serviço ou à operação (conforme exemplos apresentados no Anexo n.º 1 deste normativo).
3. No essencial, a política de aceitação de clientes deve integrar, sem limitar, o seguinte:

a) Proibição de abertura de contas anónimas ou fictícias;
b) Proibição de abertura de contas numeradas;
c) Categorização do cliente consoante a avaliação de risco efectuada;
d) Documentação necessária, informações adicionais a serem exigidas e medidas aplicáveis para cada categoria de cliente, tendo por base a avaliação de risco efectuada;
e) Medidas de diligência reforçadas para aceitação de clientes de alto risco (conforme exemplos, meramente indicativos, constantes do Anexo 2);
f) Proibição de abertura ou encerramento de conta quando a instituição financeira esteja incapaz de aplicar as medidas de diligências;
g) As circunstâncias nas quais ao cliente seja permitido agir em nome de outrem (pessoa física ou entidade) devem estar claras e de acordo com a legislação em vigor;
h) Tipo de averiguações necessárias, antes de abertura da conta, de modo a verificar se o cliente não possui antecedentes criminais, não se encontra na lista de terroristas ou organizações terroristas.

SECÇÃO III

Procedimentos de identificação e verificação de clientes

SUBSECÇÃO I

Procedimentos gerais

1. As instituições financeiras devem identificar os seus clientes nos termos e situações previstas na Lei n.º 14/2013, de 12 de Agosto, e sempre que careçam de informações suficientes e actuais sobre o cliente.

2. As instituições financeiras devem identificar e verificar a identidade e o endereço actual dos seus clientes e perceber a natureza dos seus negócios do cliente, as suas fontes de rendimento, situação financeira e a qualidade com que pretendam estabelecer a relação de negócio com a instituição.

3. As instituições financeiras devem assegurar, tanto quanto possível, que estão a lidar com uma pessoa idónea e verificar a identidade da pessoa em causa, em conformidade com as disposições do presente Capítulo. Se os fundos a serem depositados ou transferidos estiverem a ser fornecidos por uma terceira pessoa, a instituição deve proceder à identificação e verificação desta terceira pessoa. Se a instituição não for capaz de determinar se o requerente, no negócio, está a agir por conta própria ou a mando de um terceiro, deve considerar a apresentação de comunicação de operação suspeita ao GIFiM.

4. As instituições financeiras devem exigir que os clientes forneçam, por escrito, a identidade e informações da(s) pessoa(s) física(s) beneficiária(s) efectiva(s) da relação de negócio ou transacção, como parte de medidas de vigilância para identificar e verificar a identidade do(s) mesmo(s).

5. As instituições financeiras devem obter todas as informações necessárias para confirmar a identidade do cliente e para verificar a informação por este prestada. Para o efeito, poderá usar informações públicas nacionais e internacionais disponíveis, cruzar informações com outros elementos de prova, nomeadamente factura de fornecimento de serviços de água, energia, telefone, listas telefónicas, centrais de registo de crédito, registos criminais, e manter em seus arquivos.

6. No caso de o cliente não ser o beneficiário da relação de negócio, a instituição deve tomar medidas razoáveis para verificar a identidade do beneficiário efectivo, usando informações ou dados relevantes obtidos a partir de uma fonte que considere idónea para a confortar.

7. Quando um cliente encerre uma conta e solicite a abertura de outra na mesma instituição, não fica dispensado o dever de identificação e verificação e, neste caso, os detalhes sobre o arquivo do cliente devem ser reconfirmados. Os detalhes das contas e as diligências anteriormente efectuadas para verificar a identidade e os registos efectuados devem ser transferidos para os registos da nova conta.

8. Qualquer alteração posterior do nome do cliente, do seu endereço ou da informação sobre a sua situação laboral de que a instituição tenha conhecimento deve ser registada e devidamente fundamentada por prova documental, como parte do processo de medidas de diligências. A informação relativa ao cliente e ao beneficiário efectivo deve ser conservada em arquivo.

9. No caso de um cliente proceder à transferência do saldo de uma conta que ele tenha mantido com um banco para uma outra instituição, a instituição receptora deve considerar a possibilidade de o gestor de contas anterior possuir suspeitas sobre as actividades do cliente. Se a instituição receptora tiver qualquer razão para suspeitar que o cliente tenha sido rejeitado por outra instituição financeira, deve aplicar procedimentos de diligência reforçada antes de o aceitar.

10. As instituições financeiras devem, no caso de contas individuais, assegurar que as provas de identidade sejam obtidas durante o curso de uma entrevista com o cliente, de modo a certificar se o cliente é realmente a pessoa que ele afirma ser, ou seja, apurar a semelhança entre a pessoa e a fotografia que conste do documento de identidade.

11. No caso de contas conjuntas, as instituições financeiras devem verificar os nomes e endereços de todos os titulares das contas.

12. Os procedimentos de verificação necessários para estabelecer a identidade do cliente devem ser os mesmos, qualquer que seja o tipo de conta (por exemplo, conta corrente, de depósito, entre outras).

13. O nome do funcionário da instituição que conduziu o processo de abertura da conta e do responsável superior que autorizou a abertura da conta devem constar do arquivo do cliente.

14. As instituições financeiras devem proceder à identificação e verificação das pessoas ou entidades que detenham o controlo sobre os negócios e os bens.

15. Sempre que uma instituição financeira não possa obter todas as informações relativas às medidas de diligências necessárias, não deve abrir a conta, iniciar relações comerciais ou realizar a transacção, devendo considerar o envio da comunicação de operação suspeita ao GIFiM.

SUBSECÇÃO II

Abertura de conta de clientes individuais

Nos casos em que o cliente seja uma pessoa singular, a identificação deve ser comprovada pela apresentação de um dos documentos oficiais referidos no n.º 2 do artigo 5 do Decreto n.º 66/2014, de 29 de Outubro, tendo em atenção a categoria de risco do mesmo.

SUBSECÇÃO III

Abertura de conta de forma presencial por clientes individuais

1. A identificação de um cliente individual deve abranger o nome, a data de nascimento, o endereço físico, a natureza do negócio, a fonte de rendimento, o conhecimento sobre as transacções financeiras normais e qualquer relação de representação.

2. O nome de clientes individuais deve ser verificado, através de um documento válido, no decorrer de uma entrevista com o mesmo.

3. Para efeitos da alínea *a*) do n.º 1 do artigo 6 do Decreto n.º 66/2014, de 29 de Outubro, consideram-se elementos idóneos para confirmação do domicílio:

a) Facturas emitidas pelos serviços de fornecimento de energia, água, telefone, *internet*;
b) Informação que conste da lista telefónica;
c) Extracto recente do cartão de crédito ou débito de uma outra instituição financeira;
d) Referência bancária recente;
e) Qualquer outro documento que individualmente ou cumulativamente comprove o endereço do requerente para o negócio, nomeadamente a declaração do bairro e da entidade patronal.

SUBSECÇÃO IV

Formulários para abertura de conta de clientes individuais

1. O formulário de abertura de conta para cliente individual deve, no mínimo, conter a seguinte informação:

a) Nome;
b) Endereço permanente actual;

c) Endereço para correspondência;
d) Número de telefone e fax;
e) Data e local de nascimento;
f) Nacionalidade;
g) Ocupação e nome do empregador (se trabalhador por conta própria, a natureza do autoemprego e a respectiva confirmação);
h) Número Único de Identificação Tributária (NUIT);
i) Código de Classificador de Actividades Económicas (CAE);
j) Assinatura(s);
k) Carta abonatória da instituição bancária na qual o não residente é cliente no país de residência;
l) Autorização para a instituição financeira averiguar e obter referências sobre o cliente.

2. Ao formulário devidamente preenchido deve ser anexa uma cópia legível de documento de identificação usado e toda a documentação relativa à verificação da identidade do cliente.

SUBSECÇÃO V

Verificação da identidade nos casos de abertura de conta na forma não presencial

Antes de aceitar a relação de negócios com cliente não presencial, as instituições financeiras devem:

a) Adoptar procedimentos de identificação de clientes aplicáveis aos clientes presenciais e, logo que possível, criar condições para a entrevista;
b) Adoptar medidas de diligência reforçadas para mitigar o risco inerente (cliente não presencial).

SUBSECÇÃO VI

Abertura de conta por clientes individuais não residentes

1. Os clientes individuais não residentes que solicitem a abertura de conta a partir do exterior devem preencher um formulário de candidatura que, no mínimo, contenha a seguinte informação:

a) Nome;
b) Endereço permanente;
c) Endereço actual;
d) Número de telefone e número de fax;
e) Data e local de nascimento;
f) Nacionalidade(s);
g) Ocupação e nome do empregador (se trabalhador por conta própria, a natureza do autoemprego);
h) Número, data de emissão e data de validade do passaporte;
i) Assinatura(s);
j) Carta abonatória da instituição bancária na qual é cliente no país de residência actual;
k) Autorização para que a instituição financeira possa averiguar referências sobre o potencial cliente.

2. O formulário de inscrição, devidamente preenchido, deve ser acompanhado da cópia de passaporte válido e da informação sobre o endereço, confirmado através de original ou cópia autenticada de factura emitida por entidades prestadoras de serviços de terceiros, nomeadamente fornecedores de serviços de energia, água, telefone internet, etc.

3. Podem, ainda, ser solicitadas como medidas adicionais relacionadas com a verificação de endereço, a consulta à lista telefónica ou averiguações junto a instituições financeiras ou outras entidades no país de residência do cliente, ou ainda consultas a fontes nacionais ou internacionais que a instituição requerida considere idónea.

SUBSECÇÃO VII

Abertura de conta por pessoas colectivas

1. No processo de abertura de conta de pessoas colectivas, as instituições financeiras devem verificar:

a) A identificação dos accionistas que detenham o controlo de negócios e activos da empresa;
b) A identificação dos seus gestores seniores;
c) Identificação de todos os detentores de participação qualificada;
d) Identificação de todos os detentores de acções não nominativas de valor igual ou superior a 20%;
e) A identificação das pessoas autorizadas a representar a empresa;
f) Número Único de Identificação Tributária (NUIT);
g) Código de Classificador de Actividades Económicas (CAE);
h) Provas sobre a existência legal da empresa.

2. No processo de identificação e verificação devem ser exibidos os elementos indicados no n.º 4 do artigo 5 do Decreto n.º 66/2014, de 29 de Outubro.

3. Nos cenários de risco alto, a verificação e as consultas devem ser efectuadas mediante visita à empresa, de modo a apurar a sua existência e confirmar a finalidade económica nos termos do alvará ou junto da entidade de tutela, para apurar se a empresa continua a existir e se não terá sido ou não estará em processo de dissolução ou liquidação.

4. Tal como acontece com as contas de clientes individuais, a diligência do "conheça o seu cliente" nas contas de pessoas colectivas é um processo contínuo. Se houver mudanças na estrutura da empresa ou propriedade, ou se as suspeitas forem despertadas por uma mudança na natureza do negócio ou no perfil de pagamentos ou recebimentos por meio de uma conta de empresa, outras verificações devem ser efectuadas para determinar a razão das referidas alterações.

SUBSECÇÃO VIII

Abertura de conta por pessoas colectivas não residentes

O processo de identificação e verificação referido nos números 26 a 29 deste Capítulo é igualmente aplicável, com as necessárias adaptações, às pessoas colectivas não residentes que pretendam abrir conta a partir do exterior.

SUBSECÇÃO IX

Informação de natureza fiscal

1. As instituições financeiras devem, no momento da abertura de uma conta de depósito bancário, obter informação sobre o Número Único de Identificação Tributária (NUIT) de cada um dos respectivos titulares.

2. O Número Único de Identificação Tributária (NUIT) pode ser comprovado mediante a apresentação do original ou de cópia certificada de documento onde conste aquele número, ou através da recolha e verificação desse elemento de informação junto das entidades responsáveis pela sua gestão.

SUBSECÇÃO X

Consórcios/sociedades irregulares

1. Nos casos de empresas constituídas sob a forma de consórcios ou de empresa sem personalidade jurídica, a identificação e verificação das pessoas que detenham o controlo da empresa, dos accionistas com participação qualificada e dos seus mandatários, deve, igualmente, obedecer ao estabelecido nos n.os 26 a 29 deste Capítulo.

2. As instituições financeiras devem proceder a averiguações para confirmar a verdadeira natureza das actividades de negócio e para verificar se as actividades empresariais em causa possuem um propósito legítimo.

SUBSECÇÃO XI

Clubes e instituições de caridade

1. As instituições financeiras, antes de procederem à abertura de contas para clubes ou instituições de caridade, devem certificar a finalidade legítima da organização, solicitar uma cópia autenticada da constituição do clube ou instituição de caridade e, em caso de dúvida, efectuar uma visita às suas instalações, para conhecer a verdadeira natureza das suas actividades.

2. A identidade e a verificação das pessoas que detenham o controlo do clube ou da instituição de caridade devem ser determinadas de acordo com os procedimentos necessários para os clientes individuais.

3. As mudanças ocorridas no seio do clube ou da instituição de caridade implicam um novo dever de identificação e verificação.

SUBSECÇÃO XII

Fundações

1. A identificação e verificação de uma fundação deve, entre outros, ser efectuada nos termos que se seguem:

a) O seu nome;
b) A certidão de registo;
c) A data e o país de constituição;
d) O seu domicílio profissional;
e) O seu principal local de negócios e operações (se diferente do domicílio profissional).

2. A diligência para a verificação da fundação é efectuada, nomeadamente, mediante a certidão de registo emitida pela entidade competente, as últimas demonstrações financeiras auditadas e outras informações adicionais julgadas pertinentes.

3. Com relação às pessoas que dirigem a fundação, a identidade é requerida aos membros da gestão ou de órgão equiparado, especialmente aqueles que tenham autoridade para realizar um negócio ou para dar instruções sobre o uso ou a transferência de fundos ou bens, o fundador, o executor, o protector, o beneficiário e o administrador.

4. Se a fundação tiver fins de caridade, são-lhe aplicáveis as normas relativas à identidade de clubes e instituições de caridade, referidas na subsecção XI deste Capítulo.

SUBSECÇÃO XIII

Bancos correspondentes

1. Nas relações de negócio com bancos correspondentes, as instituições financeiras devem:

a) Reunir informações suficientes sobre os seus correspondentes, para entender a natureza dos seus negócios. Os factores a serem considerados incluem: informações sobre a gestão do correspondente, as principais actividades de negócios, a sua localização, o regime de prevenção e combate ao branqueamento de capitais e financiamento do terrorismo, bem como esforços de identificação de terceiros que utilizem os serviços correspondentes;
b) Determinar, a partir de informações públicas disponíveis, a reputação da instituição e a qualidade de regulação e supervisão da instituição, inclusive se ela foi alvo de alguma investigação ou acção relacionada com o branqueamento de capitais ou financiamento do terrorismo;
c) Avaliar os sistemas de controlo sobre a prevenção de branqueamento de capitais ou financiamento do terrorismo e verificar se os mesmos são adequados e eficazes;
d) Obter autorização do competente órgão de gestão sénior da instituição financeira em causa, antes de estabelecer novas relações de correspondência;
e) Documentar as responsabilidades de cada instituição, entre outras, em matéria de prevenção ao branqueamento de capitais ou financiamento do terrorismo;
f) No que respeita às contas correspondentes de transferência (*payable-through accounts*), as instituições financeiras devem assegurar que o banco cliente aplicou as medidas de diligência contínua relativamente ao cliente que tenha acesso directo às contas do banco correspondente, e que aquele banco se encontra habilitado a fornecer dados adequados sobre a identificação dos seus clientes, quando tal lhe for solicitado pelo banco correspondente.

2. Em particular, as instituições financeiras devem recusar-se a iniciar ou manter uma relação com o correspondente quando este não tenha presença física e não se integre num grupo financeiro regulamentado (bancos de fachada).

3. As instituições financeiras devem aplicar medidas de diligência reforçadas nos casos de uma relação de negócio ou transacções com pessoas jurídicas e instituições financeiras de países considerados pelo FATF como não cooperantes, cabendo ao Banco de Moçambique a divulgação, por circular, da referida lista.

SUBSECÇÃO XIV

Pessoas politicamente expostas (PPE)

1. Sem prejuízo das disposições constantes em outra legislação, as instituições financeiras devem:

a) Adoptar sistemas de gestão de risco adequados para determinar se um potencial cliente, um cliente existente ou o beneficiário efectivo é ou não uma PPE;
b) Desenvolver uma política clara, procedimentos de controlos internos adequados e manter-se especialmente vigilantes em relação a relações de negócio com as PPE, com pessoas e empresas que estejam claramente relacionadas ou associadas a eles ou outros clientes de alto risco.

2. Adoptar medidas razoáveis para determinar as fontes de riqueza e de recursos do cliente e beneficiários identificados como PPE. As instituições financeiras que possuam relação de negócios com clientes de países cujas informações públicas e idóneas os retratem como sendo vulneráveis à corrupção, devem identificar as PPE no país em causa e devem procurar determinar se o cliente possui ou não ligação familiar ou comercial com essas pessoas.

3. As instituições financeiras devem proceder à monitoria contínua, tendo em atenção o facto de os indivíduos poderem estabelecer conexões com as PPE após a criação da relação comercial.

4. Considerando o facto de que as PPE podem não ser inicialmente identificadas como tal, e considerando ainda que os clientes existentes podem, posteriormente, adquirir a qualidade de PPE, a instituição deve proceder a revisões regulares dos seus clientes, com a periodicidade mínima de 12 meses.

SUBSECÇÃO XV

Transferências electrónicas

1. Para garantir que o sistema de transferência electrónica não seja usado para fins ilícitos, e sem prejuízo da demais legislação aplicável, as instituições financeiras devem assegurar a existência de informações exactas do ordenante, bem como informações exigidas sobre o beneficiário. Devem, ainda, incluir em todas as transferências de fundos as mensagens relacionadas, devendo permanecer na cadeia da transferência de pagamento até ao seu destino final.

2. A informação que acompanha todas as transferências electrónicas deve incluir:

a) O nome do ordenante;
b) O número da conta do ordenante, se a conta foi usada para o processamento da operação;
c) A morada do ordenante, o número do documento de identificação nacional ou número de identificação de cliente, ou data e local de nascimento;
d) O nome do beneficiário;
e) O número de conta do beneficiário se essa conta for utilizada para o processamento da operação;
f) A instituição bancária beneficiária.

3. Nos casos de ausência de uma conta, deverá ser incluído o número de referência único da operação que permita sua rastreabilidade.

SUBSECÇÃO XVI

Transferências processadas por um intermediário

1. Sempre que as transferências de fundos sejam processadas por um intermediário e nos montantes definidos pelo n.º 3 do artigo 24 do Decreto n.º 66/2014, de 29 de Outubro, a instituição financeira que actue como intermediária na cadeia de transferências electrónicas deve assegurar que toda a informação sobre o ordenante e o beneficiário que acompanha a transferência seja conservada e, sempre que possível, incluída na mensagem gerada.

2. Caso existam limitações de ordem técnica que impeçam que a informação necessária sobre o ordenante ou o beneficiário que acompanha uma transferência electrónica internacional seja transmitida com a transferência electrónica doméstica correspondente, a instituição financeira intermediária que as recebe deve manter, durante pelo menos quinze anos, um registo de toda a informação recebida da instituição financeira ordenante ou de outra instituição financeira intermediária.

3. A instituição financeira intermediária deve adoptar medidas de controlo razoáveis para identificar as transferências electrónicas internacionais cuja informação necessária sobre o ordenante ou o beneficiário se encontre omissa.

4. A instituição financeira intermediária deve dispor de políticas e procedimentos eficazes baseados no risco, para determinar:

a) Quando deve executar, rejeitar ou suspender uma transferência electrónica cuja informação necessária sobre o ordenante ou o beneficiário se encontre omissa;
b) As actividades adequadas de acompanhamento.

5. A falta de informações completas do ordenante pode ser considerada factor de suspeita e, por consequência, a instituição financeira intermediária deve considerar a possibilidade de comunicação ao GIFiM. Em alguns casos, a instituição financeira beneficiária deve considerar restringir ou até mesmo encerrar a sua relação de negócios com instituições financeiras que não cumpram os requisitos acima.

SUBSECÇÃO XVII

Instituição financeira beneficiária

1. A instituição financeira beneficiária deve adoptar medidas para identificar as transferências electrónicas internacionais cuja informação necessária sobre o ordenante ou o beneficiário esteja omissa. Estas medidas podem incluir o acompanhamento posterior ou em tempo real, sempre que possível.

2. A instituição financeira beneficiária deve dispor de políticas e procedimentos eficazes baseados no risco, de modo a determinar:

a) Quando executar, rejeitar ou suspender uma transferência electrónica cuja informação necessária sobre o ordenante ou beneficiário esteja omissa;
b) As actividades adequadas de acompanhamento.

SUBSECÇÃO XVIII

Transferências electrónicas nacionais

1. As transferências electrónicas nacionais devem incluir informação do ordenante, tal como indicado nas transferências electrónicas internacionais, salvo se a informação puder ser disponibilizada pela instituição financeira beneficiária às autoridades competentes (GIFiM e autoridades judiciárias). Neste caso, a instituição financeira ordenante necessita apenas de incluir o número de conta ou o número de referência único da operação, desde que esse número permita identificar que a operação está associada ao ordenante ou ao beneficiário.

2. A informação referida no parágrafo anterior deve ser disponibilizada pela instituição financeira ordenante, num prazo de 3 dias úteis, após a recepção do pedido, quer da instituição beneficiária, quer das autoridades igualmente referidas no número anterior.

SECÇÃO IV

Monitoramento da conta e de transacções

1. O monitoramento contínuo é um aspecto essencial para a gestão do risco de branqueamento de capitais e financiamento do terrorismo. Deve incluir o exame das transacções realizadas no decurso da relação com o cliente para garantir que as mesmas são consentâneas com o conhecimento que a instituição financeira possui do cliente, nomeadamente perfil de negócios e risco.

2. As instituições financeiras devem assegurar que os documentos apresentados ou as informações recolhidas no âmbito das medidas de diligências, são conservados de forma actualizada e são relevantes para a reconstituição da transacção. O apuramento da relevância é efectuado, através da realização de revisões dos registos existentes e da análise das transacções, especialmente para as categorias de clientes ou relações comerciais de risco mais elevado.

3. O monitoramento deve estar em concordância com a avaliação de risco. Para todas as contas, as instituições financeiras devem ter sistemas para detectar padrões complexos, incomuns ou transacções suspeitas. Alguns tipos de transacções podem alertá-las sobre a possibilidade de actos de branqueamento de capitais e financiamento do terrorismo. Exemplos de actividades suspeitas podem ser aprofundados, através da consulta às tipologias de branqueamento de capitais ou financiamento do terrorismo publicados pelo FATF/GAFI em *http://www.fatf-gafi.org*, e do Anexo 3 deste normativo.

4. As instituições financeiras devem intensificar o monitoramento das contas de maior risco, devendo estabelecer indicadores-chave para essas contas, tomando por base a informação conhecida do cliente, como por exemplo, o país de origem, a(s) fonte(s) de recursos, o tipo de transacções envolvidas e outros factores de risco.

5. As instituições financeiras devem assegurar que dispõem de sistemas de informação de gestão adequados para fornecer aos gestores e OCOS, bem assim informações actualizadas necessárias para identificar, analisar e monitorar as contas.

SECÇÃO V

Inovações financeiras

1. As instituições financeiras devem adoptar as políticas ou medidas necessárias para prevenir o uso indevido de desenvolvimentos tecnológicos em esquemas de branqueamento de capitais e de financiamento do terrorismo. Devem identificar, avaliar e compreender os riscos de branqueamento de capitais e financiamento do terrorismo associados a todos os produtos (novos ou pré-existentes), serviços e canais de distribuição, e da utilização de novas tecnologias.

2. As instituições financeiras devem realizar a avaliação de risco antes da introdução de tais produtos, serviços, canais de entrega e tecnologias, e devem aplicar as medidas necessárias para gerir eficazmente os riscos de branqueamento de capitais e de financiamento do terrorismo associados.

CAPÍTULO IV

Conservação de documentos

SECÇÃO I

Registos de identidade

1. Toda a documentação exigida pelas instituições financeiras, nos termos do presente normativo e demais legislação aplicável, para verificar a identidade dos clientes e dos beneficiários efectivos deve ser conservada por um período, nunca inferior a 15 anos após o encerramento da conta ou cessação da relação de negócio com o cliente em questão.

2. Se se optar pelos serviços de um terceiro para realizar a verificação de procedimentos de identidade ou a confirmar a identidade, a conservação de documentos deve ser efectuada nos termos do número anterior.

SECÇÃO II

Registos de transacções

Os registos de transacções, independentemente da forma como são utilizados, devem ser conservados por um período não inferior a quinze anos, após a conclusão das operações em causa, de forma a auxiliar na investigação de casos de suspeita de branqueamento de capitais e financiamento do terrorismo, e devem incluir o seguinte:

a) Volume de negócio efectuado através da conta;
b) Origem dos fundos, incluindo todos os detalhes do cliente;
c) A forma em que os fundos foram creditados ou debitados da conta;
d) A identidade da pessoa que efectua a operação e a identidade do beneficiário efectivo;
e) Detalhes da contraparte;
f) O destino dos fundos;
g) A forma de instrução;
h) A data da transacção;
i) O tipo e o número de identificação de qualquer conta envolvida na transacção;
j) Qualquer outra informação que possibilite a reconstituição da transacção.

SECÇÃO III

Relatório de comunicação de operações suspeitas

1. Cada instituição financeira deverá ser registada no sistema informático do GIFiM, passando a ter um número de registo e uma senha de acesso ao formulário, a ser atribuído ao OCOS.

2. Cada comunicação de transacção suspeita enviada ao GIFiM, através do formulário, manual ou electrónico, deverá ter o seguinte conteúdo:

a) Instituição financeira que envia a comunicação;
b) Número da conta bancária envolvida na transacção;
c) Titular da conta;
d) Executor da transacção;
e) Valor monetário da transacção;
f) Descrição resumida da natureza da transacção e todas as circunstâncias que motivaram a suspeita;
g) A relação de negócio entre o suspeito e a instituição financeira;
h) Quando o suspeito seja cliente interno do banco (i.e., funcionário), deverá buscar-se informação sobre se o suspeito ainda é ou não funcionário da instituição financeira;
i) Qualquer declaração voluntária sobre a origem, fonte ou destino dos recursos;
j) O impacto da actividade suspeita na credibilidade da instituição ou pessoa que comunica;
k) Nome e assinatura do oficial de comunicação de operação suspeita.

3. O relatório interno elaborado sobre a prevenção do branqueamento de capitais e financiamento do terrorismo, as comunicações de operações suspeitas, as transacções em numerário, as transacções electrónicas de fundos e em cheque remetidas ao GIFiM devem ser conservados por um período não inferior a quinze anos após a data da respectiva elaboração.

4. Todas as conclusões relativas a transacções complexas, não comuns, suspeitas ou outras que, não tendo aquelas características, façam parte das transacções a serem comunicadas ao GIFiM, devem ser mantidas, por um período não inferior a 15 anos, contados da data da respectiva constatação.

SECÇÃO IV

Conservação da informação relativa às investigações em curso

Os registos relacionados com investigações em curso devem ser mantidos até que seja confirmado pelas autoridades competentes que o caso foi encerrado.

SECÇÃO V

Conservação das transacções efectuadas por meios electrónicos

Os registos de pagamentos electrónicos e respectivas mensagens devem ser tratados nos termos referidos nos números anteriores deste Capítulo.

CAPÍTULO V

Reconhecimento e comunicação de operações suspeitas

SECÇÃO I

Reconhecimento de operações suspeitas

1. Os funcionários das instituições financeiras devem receber capacitação e orientação suficientes para reconhecer as operações

suspeitas (ver capítulo VI sobre "Selecção e Formação"). As perguntas a serem consideradas para determinar se uma transacção é suspeita, podem ser, e sem limitar, as seguintes:

a) O volume/montante da transacção está de acordo com as actividades normais do cliente?
b) A operação é racional, no contexto do negócio do cliente ou de actividades pessoais?
c) O padrão de operações realizadas pelo cliente mudou?
d) Quando a transacção seja internacional, existe razão óbvia para que o cliente realize negócios com o país envolvido?

2. No processo de actualização dos procedimentos internos, a instituição financeira deve sempre considerar os factos e circunstâncias que deram origem a relatórios de transacções suspeitas.

SECÇÃO II

Reporte de transacções suspeitas

Todas as instituições financeiras devem assegurar:

a) Que os funcionários, nos seus postos de trabalho, saibam a quem reportar as transacções suspeitas;
b) Que a cadeia de comunicação seja clara, de modo que as suspeitas sejam repassadas de forma directa e imediata ao OCOS.

SECÇÃO III

Oficial de Comunicação de Operações Suspeitas

1. As funções e atribuições do OCOS encontram-se referidas no número 2 do Capítulo I deste normativo. Entretanto, em caso de necessidade de substituição do OCOS, por ausência ou outro motivo, a instituição financeira deve garantir que a sua substituição seja apropriada e, em nenhum caso, por um membro da Auditoria Interna, sob pena de se criar um conflito de interesses.

2. O OCOS deve ser dotado de alto grau de responsabilidade e independência. Ele é responsável por determinar se a informação ou outros assuntos contidos no relatório de transacção que recebeu gera suspeita razoável de que um cliente possa estar envolvido em actos de branqueamento de capitais e/ou financiamento do terrorismo.

3. No julgamento, o OCOS deve considerar todas as informações relevantes disponíveis sobre a pessoa ou empresa a quem o relatório inicial se refira. Tal pode incluir a necessidade de se proceder à revisão de outros padrões de transacções e dos volumes, através da conta ou contas no mesmo nome, da duração da relação de negócio e dos registos de identificação efectuados. Se, depois de concluir esta revisão, decidir que existem factos suspeitos, deve imediatamente comunicar ao GIFiM.

4. O OCOS deve agir de forma honesta e razoável e deve formular o seu juízo na base de boa-fé.

SECÇÃO IV

Procedimento de relatórios internos

1. O canal de comunicação de transacções suspeitas, para garantir rapidez e sigilo, deve ser o mais curto possível, com um número mínimo de intervenientes entre o funcionário que detecta a suspeita e o OCOS.

2. Todas as transacções suspeitas comunicadas ao OCOS devem ser documentadas. O funcionário que detecta a suspeita pode primeiro discutir com o OCOS e, em seguida, preparar o relatório inicial e enviá-lo. O relatório deve incluir detalhes completos do cliente, o seu perfil, extractos de contas, se necessário, e o relato completo quanto possível dos motivos que deram origem à suspeita.

3. O OCOS deve acusar a recepção do relatório. Todas as investigações internas feitas em relação ao relatório, bem assim a razão que determinou o envio ou não do relatório ao GIFiM, devem ser documentadas. Esta informação pode ser necessária para completar o relatório inicial ou como evidência de boas práticas, se, em algum momento futuro, houver uma investigação sobre um caso que o OCOS tenha optado por não comunicar, vindo posteriormente as suspeitas a confirmar-se.

SECÇÃO V

Relatório de operações suspeitas

O formato padrão de comunicação de operações suspeitas é concebido e definido pelo GIFiM, devendo todas as instituições financeiras agir nos termos determinados por este.

CAPÍTULO VI

Selecção e formação de trabalhadores

SECÇÃO I

Selecção de funcionários

As instituições financeiras devem, na sua política de contratação, adoptar procedimentos de verificação, de modo a garantir um elevado padrão na contratação de funcionários. A este respeito, deve procurar obter referências apropriadas na altura do recrutamento.

SECÇÃO II

Formação de trabalhadores

SUBSECÇÃO I

Programa de formação contínua

As instituições financeiras devem, no intuito da prevenção do branqueamento de capitais e financiamento do terrorismo, implementar um programa de formação contínua para os seus funcionários, no que concerne a programas de gestão de risco e práticas com vista a cumprir parte do seu dever legal de tomar medidas razoáveis nesse sentido.

SUBSECÇÃO II

Requisitos para diferentes categorias de funcionários

1. Todo o pessoal deve receber formação sobre a prevenção e combate ao branqueamento de capitais e financiamento do terrorismo, relativa ao quadro legal e regulamentar vigente em Moçambique, sobre os normativos internacionais que regulem a matéria e sobre as tendências e os desenvolvimentos no que respeita às práticas de branqueamento de capitais e financiamento do terrorismo.

2. Todos os funcionários devem igualmente receber formação sobre a avaliação e gestão de risco.

3. Os funcionários com responsabilidade de abertura de conta e aceitação de novos clientes devem receber formação no que diz respeito à identificação e aos procedimentos de verificação da identidade dos clientes. Devem igualmente estar familiarizados com o reconhecimento e manuseio de transacções suspeitas, assim como com os procedimentos de comunicação de operações suspeitas internas.

4. Os funcionários do *front-office* devem receber formação para conhecer a verdadeira identidade do cliente e conhecer o suficiente sobre o tipo de actividades comerciais esperadas do cliente, para que estejam atentos a qualquer mudança no padrão das suas transacções ou a circunstâncias que possam constituir conduta criminosa. Estes funcionários devem igualmente receber

formação sobre o reconhecimento e manuseio de operações suspeitas, bem como sobre os procedimentos a serem adoptados quando uma transacção é considerada suspeita.

5. Os funcionários que procedam a transferências electrónicas devem receber formação sobre a prevenção do branqueamento de capitais e financiamento do terrorismo, e sobre as medidas preventivas a estas aplicáveis.

6. Os funcionários recém-admitidos devem, logo que possível, beneficiar de formação geral sobre a prevenção ao branqueamento de capitais e financiamento do terrorismo, e sobre os procedimentos internos adoptados para o reporte de operações suspeitas. Devem, igualmente, ter acesso a toda a legislação e às políticas e procedimentos da instituição sobre a prevenção do branqueamento de capitais e financiamento do terrorismo.

7. Os membros de conselhos de administração e demais gestores das instituições financeiras devem receber formação sobre todos os aspectos do processo de branqueamento de capitais e financiamento do terrorismo. Entre outros conteúdos, a formação deve incluir políticas de gestão de risco, sanções decorrentes da Lei nos casos de não-comunicação, exclusão de responsabilidades em casos de reporte, procedimentos de comunicação interna, requisitos para a verificação da identidade, manutenção de registos e alocação de recursos para prevenção.

8. Para além da capacitação geral sobre a prevenção do branqueamento de capitais e financiamento do terrorismo, o OCOS deve beneficiar de formação sobre todos os aspectos da inteligência financeira, as políticas internas aplicáveis em suas instituições e o reconhecimento de transacções suspeitas, instrução inicial e contínua sobre a validação e comunicação de operações suspeitas, sobre o regime de retorno da informação suspeita encaminhada e sobre as novas tipologias e tendências deste tipo de crime.

SUBSECÇÃO III

Curso de reciclagem

As instituições financeiras devem anualmente garantir formação para que os seus funcionários não se esqueçam das suas responsabilidades.

SUBSECÇÃO IV

Registos

As instituições financeiras devem manter o registo de todas as formações concedidas aos seus funcionários, incluindo o conteúdo, os beneficiários e a entidade que as facilitou.

CAPÍTULO VII

Listas Designadas

Os OCOS devem consultar numa base permanente, as Listas Designadas de sanções estabelecidas pelas Resoluções 1267, de 1999 e 1989, de 2011 do Conselho de Segurança das Nações Unidas, e solicitar à autoridade competente, o congelamento sem demora das contas constantes dessa lista ou interromper qualquer relação de negócio com titulares de tais contas.

ANEXO 1 – Avaliação de Risco

O presente Anexo visa apresentar alguns exemplos sobre a avaliação de risco. Contudo, a sua aplicação não é considerada obrigatória, cabendo a cada instituição financeira aferir a utilidade deste instrumento no contexto da sua política e dos seus procedimentos de gestão de risco.

I. Circunstâncias exemplificativas para avaliação de risco de branqueamento de capitais e financiamento do terrorismo:

1) Os riscos de branqueamento de capitais e de financiamento do terrorismo podem ser, sem limitar, os seguintes:

a) Risco cliente;
b) Risco país ou geográfico;
c) Risco associado ao produto, aos serviços, à operação ou ao canal de pagamento.

2) As categorias de risco de branqueamento de capitais e financiamento do terrorismo, sem limitar, podem ser:

a) Risco baixo;
b) Risco moderado;
c) Risco alto.

II. Exemplo de diferentes categorias de riscos

1) Cliente de <u>risco elevado</u>:

a) A relação de negócios decorre de forma invulgar (exemplo, uma significativa e inexplicada distância geográfica entre a instituição e o cliente);
b) Clientes não residentes;
c) Pessoa politicamente exposta;
d) Pessoas colectivas ou entidades sem personalidade jurídica que sejam estruturadas de detenção de activos pessoais;
e) Sociedade com accionistas por conta de outra pessoa ou acções ao portador;
f) Actividades que tenham necessidade de fontes de financiamento consideráveis;
g) A estrutura da propriedade da sociedade parece ser invulgar ou excessivamente complexa, dada a natureza da actividade da sociedade.

2) Cliente de <u>risco baixo</u>

a) As instituições financeiras implementam eficazmente as obrigações de prevenção e combate ao branqueamento de capitais e financiamento do terrorismo;
b) As sociedades estão cotadas num mercado bolsista e sujeitas a deveres de informação que visam garantir transparência adequada aos beneficiários efectivos;
c) Administrações ou empresas públicas. Porém, tais entidades não devem necessariamente ser consideradas de risco baixo: dependendo das jurisdições, as administrações ou empresas públicas podem ser de risco alto. Por exemplo, as empresas estatais a partir de um país considerado de altos índices de corrupção.

3) Risco país ou geográfico elevado

a) Os países identificados por fontes idóneas, por exemplo, os relatórios de avaliação mútua ou de avaliação pormenorizada ou relatórios de acompanhamento publicados, como não dispondo de sistemas adequados de prevenção e combate ao branqueamento de capitais e financiamento do terrorismo;
b) Países sujeitos a sanções, embargos ou medidas análogas impostas, por exemplo, as sanções da Organização das Nações Unidas - ONU (sanção por parte do Conselho de Segurança);
c) Países identificados por fontes idóneas como sendo caracterizados por níveis consideráveis de corrupção ou outra actividade criminal;
d) Países ou zonas geográficas identificados por fontes idóneas como proporcionando fundos ou apoio a actividade terroristas, ou nos quais operem organizações terroristas designadas.

4) Risco país ou geográfico baixo

a) Os países identificados por fontes idóneas como, por exemplo, os relatórios publicados de avaliação mútua, pormenorizada, ou de acompanhamento, como dispondo de sistemas eficazes de branqueamento de capitais e financiamento do terrorismo;

b) Países identificados por fontes idóneas como sendo caracterizados por níveis reduzidos de corrupção ou outra actividade criminal.

5) Risco alto associado ao produto, serviço, operação ou canal de distribuição:

a) Banca privada (serviços corporate, banca à distância);

b) Relações de negócio ou operações sem a presença física do cliente;

c) Pagamento recebido de terceiros desconhecidos ou não associados.

6) Risco baixo associado ao produto, serviço, operação ou canal de distribuição

Produtos ou serviços financeiros que proporcionem serviços limitados e definidos de modo pertinente, com vista a aumentar o acesso a determinados tipos de clientes para fins de inclusão financeira.

ANEXO 2 — Medidas de Diligência Contínua

1. As instituições financeiras podem implementar, consoante a categoria de risco envolvida, os seguintes tipos de medidas de diligência:

a) **Medidas de diligência simplificadas:** medidas de diligências menos rigorosas comparativamente às medidas de diligência básicas, que apenas podem ser aplicadas quando o grau de risco seja reduzido. As medidas de diligências simplificadas devem ser proporcionais aos factores de baixo risco.

As medidas simplificadas não devem ser aplicáveis quando exista suspeita de actos de branqueamento de capitais e de financiamento do terrorismo.

b) **Medidas de diligência reforçadas:** Quaisquer medidas de diligência adicionais empreendidas para além das diligências básicas. Elas são realizadas para todos os clientes de alto risco.

2. Exemplo de medidas de diligências reforçadas:

a) Obtenção de informações adicionais sobre o cliente (profissão, bens, informações disponíveis em bases de dados nacionais, ou internacional, na internet, etc.) e a actualização regular, no intervalo mínimo de 12 meses, da informação de identificação do cliente e do beneficiário efectivo;

b) Obtenção de informações adicionais sobre a natureza da relação de negócio;

c) Obtenção de informação sobre os motivos das operações pretendidas ou realizadas;

d) Obtenção de autorização do Conselho de Administração ou órgão equiparado para iniciar ou continuar a realização de negócio;

e) Aumento da frequência dos controlos e selecção do tipo de operações que necessitem de um exame mais profundo;

f) Obrigação de efectuar o primeiro pagamento, através de uma conta aberta em nome do cliente, a partir de um outro banco sujeito a normas de diligência semelhante.

3. Exemplos de medidas de diligência simplificadas (medidas simplificadas):

a) Verificação da identidade do cliente e do beneficiário efectivo após o estabelecimento da relação de negócio;

b) Redução da frequência das actualizações dos elementos de identificação do cliente;

c) Redução da intensidade da vigilância contínua e da profundidade do exame e das operações;

d) Não recolher informações específicas nem implementar medidas específicas que permitam compreender o objecto e a natureza da relação de negócio, mas inferir o objecto e a natureza do tipo de transacção efectuada ou relação de negócio estabelecida.

ANEXO 3 — Exemplos de Transacções Suspeitas Referentes a Actos de Branqueamento de Capitais e Financiamento do Terrorismo

Nota:

Nenhum dos factores a seguir exemplificados, de forma isolada, significa necessariamente que um cliente ou terceiro está envolvido em actos de branqueamento de capitais e financiamento do terrorismo. No entanto, na maioria dos casos uma combinação dos factores abaixo pode despertar suspeitas. Em qualquer caso, o que poderá ou não dar origem a uma suspeita dependerá de circunstâncias particulares.

1. Exemplos de transacções suspeitas - branqueamento de capitais

1.1 Branqueamento de capitais, através de transacções em numerário

a) Depósitos à vista em montantes elevados feitos por um indivíduo ou empresa que, pelo tipo de negócio ou actividades que desenvolva, normalmente, seriam efectuados por cheques e outros instrumentos;

b) Aumentos substanciais nos depósitos em numerário de qualquer pessoa ou empresa, sem causa aparente, especialmente se tais depósitos são posteriormente transferidos dentro de um curto período de tempo para outra conta e/ou para um destino que normalmente não tem ligação com o cliente;

c) Cliente que efectua vários depósitos em numerário em montantes considerados normais (abaixo do limite estabelecido nas alíneas *a*) e *b*) do n.º 3 do artigo 18 da Lei n.º 14/2013, de 12 de Agosto), mas que no final totaliza montantes significativos;

d) Contas de empresas cujas operações, depósitos e levantamentos, sejam em numerário em vez de nas formas de movimentos normalmente associados às operações comerciais de uma empresa (por exemplo, cheques, cartas de crédito, letras de câmbio, etc.);

e) Cliente que constantemente pague ou deposite dinheiro para cobrir pedidos de transferências bancárias, conta corrente ou outros instrumentos monetários negociáveis e facilmente comercializáveis;

f) Cliente que constantemente solicite a troca de grandes quantidades de notas de baixa denominação para as de maior denominação;

g) Troca (compra) frequente de dinheiro em outras moedas;

h) Agências/Filiais com muitas mais transacções em numerário do que o habitual.

1.2 Branqueamento de capitais usando contas bancárias

a) Cliente que deseje manter e administrar um número de contas não compatível com o seu tipo de negócio ou transacções;

b) Cliente que possua inúmeras contas bancárias e em cada uma delas, quantias em dinheiro consideradas normais para o seu perfil, mas cujo saldo total o saldo extravase o seu perfil financeiro;

c) Qualquer pessoa ou empresa cuja conta bancária aponte para um perfil normal de negócio, mas seja usada para receber ou desembolsar grandes somas sem finalidade óbvia nem relação com o titular da conta e/ou com o seu negócio;

d) Solicitação de pagamento de cheques de terceiros em grandes montantes, endossados a favor do cliente;

e) Levantamento em numerário de uma conta previamente dormente/inactiva, ou a partir de uma conta que acabe de receber um elevado crédito do exterior;

f) Cliente que use várias agências para realizar transacções em numerário e operações cambiais;

g) Uso frequente de representantes, evitando o contacto com a instituição financeira;

h) Aumentos substanciais nos depósitos em numerário ou instrumentos negociáveis por uma empresa, usando contas de clientes ou de empresa, especialmente se os depósitos forem prontamente transferidos para outro cliente ou empresa;

i) Cliente que recuse fornecer informações que, em circunstâncias normais, seriam úteis para a sua elegibilidade a crédito ou outros serviços bancários.

j) Uso insuficiente das facilidades bancárias normais (por exemplo, recusas de oferta de altas taxas de juros em razão do montante do saldo existente);

k) Pagamentos efectuados por um grande número de indivíduos na mesma conta, sem uma explicação adequada.

1.3 Branqueamento de capitais através de uma actividade internacional *offshore*

a) Uso de cartas de crédito e outros métodos de financiamento ao comércio exterior para movimentar dinheiro entre os países onde esse comércio não é compatível com o negócio habitual do cliente;

b) Clientes que façam pagamentos regulares e em montantes elevados, incluindo transferências electrónicas, não claramente identificados como transacções de boa-fé, ou clientes que recebam pagamentos regulares em montantes elevados provenientes de países que são comummente associados com a produção, transformação ou comercialização de drogas, organizações terroristas ou prática de qualquer um dos crimes conexos referidos no artigo 7 da Lei n.º 14/2013, de 12 de Agosto;

c) Existência de grandes saldos não consistentes com o conhecimento do volume de negócios do cliente e posterior realização de transferências para conta (s) no exterior;

d) Transferências electrónicas de fundos inexplicáveis por parte dos clientes, usando os serviços de transferência de dinheiro ou similares;

e) Pedidos frequentes de emissão de cheques de viagem, saques em moeda estrangeira ou outros instrumentos negociáveis.

1.4 Branqueamento de capitais envolvendo funcionários de instituições financeiras

a) Alterações nas características dos empregados (por exemplo, estilos de vida luxuosos);

b) Mudanças no desempenho do funcionário ou agente (por exemplo, vendedor de produtos com aumento notável ou inesperado no seu desempenho).

c) Efectivação de transacções sem que se revele a identidade do beneficiário efectivo;

d) Esquemas de sobrefacturação, em que os materiais encomendados para uma compra são de baixa qualidade e os preços maiores que o estipulado, sem que tal se reflicta no contrato negociado.

1.5 Branqueamento de capitais com recurso a financiamentos garantidos e não garantidos

a) Clientes que reembolsem empréstimos de forma inesperada;

b) Pedido de financiamento contra activos detidos pela instituição ou por um terceiro, onde a origem dos bens não seja razoavelmente conhecida ou os bens sejam incompatíveis com a posição do cliente;

c) Pedido de financiamento cuja fonte de recursos para o reembolso nos termos do acordo não esteja clara.

1.6 Relação negocial

a) Clientes que sem nenhuma razão discernível usem os serviços da empresa, por exemplo, clientes com endereços distantes que poderiam encontrar o mesmo serviço mais próximo das suas residências;

b) Clientes cujos requisitos não estejam no padrão normal dos negócios da empresa, que poderiam ser mais facilmente atendidos em outro lugar;

c) Um investidor introduzido por uma instituição financeira sedeada no exterior, baseados em países com conotação de produção de drogas, tráfico de drogas, ou outro crime conexo referido no artigo 7 da Lei n.º 14/2013, de 12 de Agosto;

d) Qualquer transacção em que a contraparte da operação seja desconhecida.

1.7 Intermediários

Qualquer uso aparentemente desnecessário de um intermediário numa transacção deve dar origem a um inquérito complementar.

1.8 Recurso ao sigilo como fundamento para ocultar alguma informação pode despertar suspeitas:

a) Zelo excessivo ou desnecessário do potencial cliente;

b) Concessão desnecessária de amplos poderes na procuração;

c) Falta de vontade de divulgar as fontes de recursos;

d) Atraso e/ou falta de vontade de revelar a identidade dos beneficiários efectivos.

1.9 Factores de suspeitas na actuação de empresas:

a) As empresas que mantenham a continuidade da sua actividade mesmo com perdas substanciais;

b) As estruturas de grupo complexas, sem uma causa aparente;

c) A rotatividade frequente de accionistas, directores ou administradores, sem causa aparente;

d) Estrutura de grupo rentável para efeitos fiscais;

e) Uso de contas bancárias em várias moedas, sem motivo aparente;

f) A existência de transferências inexplicáveis de grandes somas de dinheiro, através de várias contas bancárias;

g) Administração ou gestão fraudulenta; em prejuízo dos interesses da própria empresa.

2. Exemplos de operações suspeitas – financiamento do terrorismo

2.1 Contas

a) Conta inactiva com saldo mínimo, mas que, de repente, recebe um depósito ou uma série de depósitos, seguidos de levantamentos diários até ao limite do montante depositado;

b) Ao abrir uma conta, o cliente furta-se a prestar as informações requeridas pela instituição financeira, ou presta declarações falsas ou de difícil verificação;

c) Conta sobre a qual, várias pessoas possuam poderes para assinar, aparentando tais pessoas, no entanto, não ter qualquer relação entre si (qualquer vínculo familiar ou relacionamento de negócios);

d) Conta aberta em nome de uma pessoa jurídica, uma associação ou fundação, que pode estar ligada a uma organização terrorista e que apresente os movimentos de saldo acima do nível declarado.

2.2. Depósitos e levantamentos

a) Conta de empresa a partir da qual sejam normalmente privilegiados levantamentos em numerário em detrimento de outros meios de pagamentos;

b) Depósito de elevados montantes efectuado em numerário para a conta de uma pessoa física ou jurídica, quando a actividade empresarial aparente do indivíduo ou entidade seria normalmente realizada em cheque ou outros instrumentos de pagamento;

c) Mistura de depósitos em numerário e instrumentos monetários em uma conta em que tais operações não pareçam ter qualquer relação com o uso normal da conta;

d) Várias transacções realizadas no mesmo dia, ou em dias consecutivos, em várias agências da instituição financeira, que indiciem uma tentativa de despiste;

e) Depósitos ou levantamentos em numerário, de forma consecutiva e em quantias que se encontrem abaixo do limite de reporte ao GIFiM.

2.3 Transferências electrónicas

a) Transferência bancárias ordenadas em pequenos montantes, em dias consecutivos ou intercalados, estando evidente um aparente esforço para evitar a submissão de relatórios ao GIFiM;

b) Transferência bancária em ausência de informações sobre o remetente ou a pessoa em nome da qual a transacção é realizada, quando a inclusão de tais informações seria de se esperar;

c) Uso de várias contas, nomeadamente pessoal, de empresa, de organismos ou instituições de caridade para recolher fundos e remeter imediatamente ou após um curto período de tempo para um pequeno número de beneficiários estrangeiros;

d) Operações cambiais realizadas em nome de um cliente por um terceiro, seguidas de transferências electrónicas de fundos para locais que não tenham relação comercial aparente com o cliente ou para países considerados não cooperantes.

2.4 Características do cliente ou da actividade

a) Partilha de endereço por indivíduos envolvidos em transacções em numerário, especialmente quando o endereço seja também um local de negócios e/ou não pareça corresponder à ocupação declarada (por exemplo, estudantes, desempregados, trabalhadores por conta própria, etc.);

b) Ocupação declarada pelo cliente não compatível com o nível ou tipo de transacção (por exemplo, um estudante ou um indivíduo desempregado que recebe ou envia um grande número de transferências bancárias, ou que faz levantamentos máximos de caixa diários em várias agências);

c) Transacções efectuadas por organizações sem fins lucrativos ou de caridade, nas quais não pareça haver finalidade económica ou lógica, e não pareça haver relação entre a actividade declarada da organização e as outras partes envolvidas na transacção;

d) Inconsistências inexplicáveis detectadas no processo de identificação ou verificação do cliente (por exemplo, em relação ao país de residência anterior ou actual, ao país de emissão do passaporte, a países visitados, de acordo com o registo do passaporte, e em documentos fornecidos para confirmar o nome, o endereço e a data de nascimento).

2.5 Transacções ligadas aos países ou zonas geográficas identificados por fontes idóneas como proporcionando fundos ou apoio a actividades terroristas

a) As operações envolvendo trocas de moeda estrangeira consecutivas dentro de um curto espaço de tempo, por transferências electrónicas para locais identificados por fontes idóneas como jurisdições não cooperantes;

b) Depósitos consecutivos, dentro de um curto espaço de tempo, de transferências electrónicas de fundos, especialmente para ou através de locais considerados por fontes idóneas como jurisdições não cooperantes;

c) A conta bancária que receba ou ordene um grande número de transferências electrónicas, em relação às quais pareça não haver nenhuma lógica de negócio ou outra finalidade económica, principalmente quando estas transferências se destinem ou provenham de jurisdições consideradas não cooperantes;

d) Uso de várias contas para colectar e canalizar fundos para um pequeno número de beneficiários estrangeiros, pessoas físicas e empresas, particularmente quando estes estejam em jurisdições não cooperantes;

e) Cliente que obtenha um instrumento de crédito ou se envolva em transacções financeiras comerciais com o movimento de fundos para ou a partir de jurisdições não cooperantes, quando não pareça haver razões lógicas de negócios para lidar com esses locais;

f) Abertura de contas de instituições financeiras a partir de locais de jurisdições não cooperantes;

g) Enviar ou receber fundos, através de transferências internacionais de e/ou para locais ou jurisdições não cooperantes.

Preço — 21,00 MT

IMPRENSA NACIONAL DE MOÇAMBIQUE, E.P.